

2024/1772

25.6.2024

NAŘÍZENÍ KOMISE V PŘENESENÉ PRÁVOMOCI (EU) 2024/1772**ze dne 13. března 2024,****kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, v nichž jsou upřesněna kritéria klasifikace incidentů souvisejících s IKT a kybernetických hrozeb, stanoveny prahové hodnoty významnosti a upřesněny údaje v hlášeních závažných incidentů****(Text s významem pro EHP)**

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 ⁽¹⁾, a zejména na čl. 18 odst. 4 třetí pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

- (1) Cílem nařízení (EU) 2022/2554 je harmonizovat a zjednodušit požadavky na hlášení incidentů souvisejících s IKT, jakož i provozních nebo bezpečnostních incidentů souvisejících s platbami týkajícími se úvěrových institucí, platebních institucí, poskytovatelů služeb informování o účtu a institucí elektronických peněz (dále jen „incidenty“). Vzhledem k tomu, že se požadavky na hlášení vztahují na dvacet různých druhů finančních subjektů, měly by být klasifikační kritéria a prahové hodnoty významnosti pro stanovení závažných incidentů a významných kybernetických hrozeb upřesněny jednoduchým, harmonizovaným a konzistentním způsobem, který zohlední specifika služeb a činností všech příslušných finančních subjektů.
- (2) Aby byla zajištěna proporcionalita, měla by klasifikační kritéria a prahové hodnoty významnosti odrážet velikost a celkový rizikový profil všech finančních subjektů a povahu, rozsah a složitost jejich služeb. Kritéria a prahové hodnoty významnosti by navíc měly být navrženy tak, aby se uplatňovaly jednotně u všech finančních subjektů bez ohledu na jejich velikost a rizikový profil a nepředstavovaly v souvislosti s hlášením nepřiměřenou zátěž pro menší finanční subjekty. Aby se však vyřešily situace, kdy je incidentem, který sám o sobě nepřekračuje použitelnou prahovou hodnotu, dotčen značný počet klientů, měla by být stanovena absolutní prahová hodnota určená především pro větší finanční subjekty.
- (3) V souvislosti s rámci pro hlášení incidentů, které existovaly již před vstupem nařízení (EU) 2022/2554 v platnost, by finančním subjektům měla být zajištěna kontinuita. Klasifikační kritéria a prahové hodnoty významnosti by proto měly být v souladu s obecnými pokyny EBA k hlášení závažných incidentů podle směrnice Evropského parlamentu a Rady (EU) 2015/2366 ⁽²⁾, obecnými pokyny k informacím a oznámením zásadních změn, které mají registry obchodních údajů pravidelně předkládat orgánu ESMA, rámcem jednotného mechanismu dohledu pro hlášení kybernetických incidentů přijatým Evropskou centrální bankou a dalšími příslušnými pokyny a měly by z nich vycházet. Klasifikační kritéria a prahové hodnoty by rovněž měly být vhodné pro finanční subjekty, které před vstupem nařízení (EU) 2022/2554 v platnost žádným požadavkům na hlášení incidentů nepodléhaly.
- (4) Pokud jde o klasifikační kritérium „výše a počet dotčených transakcí“, pojem transakce je široký a zahrnuje různé činnosti a služby, na které se vztahují odpovědné akty použitelné na finanční subjekty. Pro účely tohoto klasifikačního kritéria by měl pojem transakce zahrnovat platební transakce a všechny formy výměny finančních nástrojů, kryptoaktiv, komodit nebo jakýchkoli jiných aktiv, a to i ve formě marže, zajištění nebo zástavy, za hotové peníze nebo jakékoli jiné aktivum. Pro účely klasifikace by se měly brát v úvahu všechny transakce, které zahrnují aktiva, jejichž hodnotu lze vyjádřit peněžní částkou.

⁽¹⁾ Úř. věst. L 333, 27.12.2022, s. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

⁽²⁾ Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35, ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

- (5) Klasifikační kritéria by měla zajistit, aby byly zachyceny všechny relevantní typy závažných incidentů. Řada klasifikačních kritérií nemusí nutně zachytit kybernetické útoky spojené s vniknutím do sítě nebo informačních systémů. Ty jsou však významné, protože jakékoli vniknutí do sítě a informačních systémů může finančnímu subjektu způsobit újmu. Klasifikační kritéria „dotčené významné služby“ a „ztráty údajů“ by proto měla být upřesněna tak, aby zachytily tyto typy závažných incidentů, zejména neoprávněná vniknutí, která i přesto, že jejich dopady nejsou známy okamžitě, mohou mít závažné důsledky, jako je především porušení zabezpečení údajů a únik údajů.
- (6) Vzhledem k tomu, že úvěrové instituce podléhají jak rámci pro klasifikaci incidentů podle článku 18 nařízení (EU) 2022/2554, tak rámci pro operační riziko podle nařízení Komise v přenesené pravomoci (EU) 2018/959 ⁽⁹⁾, měl by být přístup k posuzování ekonomického dopadu incidentů na základě výpočtu nákladů a ztrát co nejkonzistentnější v obou rámcích, aby se zabránilo zavedení neslučitelných nebo rozporných požadavků.
- (7) Kritérium týkající se územního rozsahu incidentu stanovené v čl. 18 odst. 1 písm. c) nařízení (EU) 2022/2554 by se mělo zaměřit na přeshraniční dopad incidentu, neboť dopad incidentu na činnosti finančního subjektu v rámci jedné jurisdikce bude zachycen ostatními kritérii stanovenými v uvedeném článku.
- (8) Vzhledem k tomu, že klasifikační kritéria jsou na sobě závislá a vzájemně propojená, měl by být přístup k identifikaci závažných incidentů, které se mají hlásit v souladu s čl. 19 odst. 1 nařízení (EU) 2022/2554, založen na kombinaci kritérií, z nichž by některá kritéria, která úzce souvisí s definicí incidentu souvisejícího s IKT a definicí závažného incidentu souvisejícího s IKT stanovenými v čl. 3 bodech 8 a 10 nařízení (EU) 2022/2554, měla mít při klasifikaci závažných incidentů větší váhu než ostatní kritéria.
- (9) S cílem zajistit, aby zprávy a oznámení o závažných incidentech, které příslušné orgány obdrží podle čl. 19 odst. 1 nařízení (EU) 2022/2554, sloužily pro účely dohledu i prevence šíření nákazy do celého finančního sektoru, by prahové hodnoty významnosti měly umožňovat zachycení závažných incidentů mimo jiné zaměřením na dopad na významné služby jednotlivých subjektů, konkrétní absolutní a relativní prahové hodnoty u klientů nebo finančních protistran, transakce značící významný dopad na finanční subjekt a významnost dopadu v jiných členských státech.
- (10) Incidenty, kterými jsou dotčeny služby IKT nebo síť a informační systémy, jež podporují zásadní nebo důležité funkce, nebo finanční služby vyžadující povolení, anebo zlovolný neoprávněný přístup do sítě a informačních systémů podporujících zásadní nebo důležité funkce by měly být považovány za incidenty dopadající na významné služby finančních subjektů. Zlovolný neoprávněný přístup do sítě a informačních systémů podporujících zásadní nebo důležité funkce finančních subjektů představuje pro finanční subjekt vážná rizika, a jelikož jím mohou být dotčeny i další finanční subjekty, měl by být vždy považován za závažný incident, který se musí hlásit.
- (11) Opakující se incidenty, které k sobě váže obdobná zjevná hlavní příčina a které samostatně nepředstavují závažné incidenty, mohou být známkou podstatných nedostatků a slabých míst v postupech finančního subjektu pro řízení incidentů a rizik. Proto by opakující se incidenty v případech, že k nim dochází opakovaně po určitou dobu, měly být společně považovány za závažné incidenty.
- (12) S ohledem na to, že kybernetické hrozby mohou mít negativní dopad na finanční subjekt a finanční sektor, měly by se u významných kybernetických hrozeb, jež mohou finanční subjekty oznamovat, uvádět pravděpodobnost jejich naplnění a význam jejich potenciálního dopadu. Aby se zajistilo jasné a konzistentní posuzování významnosti kybernetických hrozeb, měla by proto klasifikace kybernetické hrozby jako významné záviset na tom, nakolik je pravděpodobné, že pokud by se hrozba naplnila, byla by splněna kritéria klasifikace incidentů jako závažných a dosaženy související prahové hodnoty, na typu kybernetické hrozby a na informacích, jež má finanční subjekt k dispozici.

⁽⁹⁾ Nařízení Komise v přenesené pravomoci (EU) 2018/959 ze dne 14. března 2018, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 575/2013, pokud jde o regulační technické normy pro upřesnění metodiky hodnocení, v jejímž rámci mohou příslušné orgány institucím povolit použití pokročilých přístupů k měření operačního rizika (Úř. věst. L 169, 6.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

- (13) Vzhledem k tomu, že se příslušným orgánům v jiných členských státech mají oznamovat incidenty, které mají dopad na finanční subjekty a zákazníky v jejich jurisdikci, mělo by posouzení dopadu v jiné jurisdikci v souladu s čl. 19 odst. 7 nařízení (EU) 2022/2554 vycházet z hlavní příčiny incidentu, z možného šíření nákazy prostřednictvím poskytovatelů z řad třetích stran a na infrastruktury finančních trhů, jakož i z dopadu incidentu na významné skupiny klientů nebo finančních protistran.
- (14) Procesy hlášení a oznamování uvedené v čl. 19 odst. 6 a 7 nařízení (EU) 2022/2554 by měly příslušným příjemcům umožnit, aby posoudili dopad incidentů. Předávané informace by proto měly zahrnovat všechny údaje obsažené v hlášeních incidentů, která předložil finanční subjekt příslušnému orgánu.
- (15) Pokud incident představuje porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679 a směrnice 2002/58/ES, neměly by být tímto nařízením dotčeny povinnosti týkající se zaznamenávání a oznamování případů porušení zabezpečení osobních údajů stanovené v uvedených právních předpisech Unie. Příslušné orgány by měly spolupracovat a vyměňovat si informace o všech relevantních záležitostech s orgány uvedenými v nařízení Evropského parlamentu a Rady (EU) 2016/679 ⁽⁴⁾ a směrnicí Evropského parlamentu a Rady 2002/58/ES ⁽⁵⁾.
- (16) Toto nařízení vychází z návrhů regulačních technických norem, které Komisi předložily evropské orgány dohledu po konzultaci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) a Evropskou centrální bankou (ECB).
- (17) Společný výbor evropských orgánů dohledu uvedený v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ⁽⁶⁾, v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ⁽⁷⁾ a v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ⁽⁸⁾ uskutečnil o návrzích regulačních technických norem, z nichž toto nařízení vychází, otevřené veřejné konzultace, analyzoval potenciální náklady a přínosy navrhovaných norem a požádal o stanovisko skupinu subjektů působících v bankovním zřízení podle článku 37 nařízení (EU) č. 1093/2010, skupinu subjektů působících v oblasti pojištění a zajištění a skupinu subjektů působících v oblasti zaměstnaneckého penzijního pojištění zřízené podle článku 37 nařízení (EU) č. 1094/2010 a skupinu subjektů působících v oblasti cenných papírů a trhů zřízenou podle článku 37 nařízení (EU) č. 1095/2010.

⁽⁴⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

⁽⁵⁾ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

⁽⁶⁾ Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovníctví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁽⁷⁾ Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES (Úř. věst. L 331, 15.12.2010, s. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁽⁸⁾ Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

- (18) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ⁽⁹⁾ byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 24. ledna 2024,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

KLASIFIKAČNÍ KRITÉRIA

Článek 1

Klienti, finanční protistrany a transakce

1. Počet klientů dotčených incidentem uvedený v čl. 18 odst. 1 písm. a) nařízení (EU) 2022/2554 odráží počet všech dotčených klientů, ať už fyzických či právnických osob, kteří během incidentu nemohou nebo nemohli využívat služby poskytované finančním subjektem nebo na které měl incident nepříznivý dopad. Do tohoto počtu se zahrnou rovněž třetí strany, na které se jakožto na příjemce dotčené služby výslovně vztahuje smluvní ujednání mezi finančním subjektem a klientem.
2. Počet finančních protistran dotčených incidentem uvedený v čl. 18 odst. 1 písm. a) nařízení (EU) 2022/2554 odráží počet všech dotčených finančních protistran, které s finančním subjektem uzavřely smluvní ujednání.
3. Pokud jde o význam klientů a finančních protistran dotčených incidentem uvedený v čl. 18 odst. 1 písm. a) nařízení (EU) 2022/2554, zohlední finanční subjekt rozsah, v němž dopad na klienta nebo finanční protistranu ovlivní plnění obchodních cílů finančního subjektu, a potenciální dopad incidentu na tržní efektivitu.
4. Pokud jde o výši nebo počet transakcí dotčených incidentem uvedené v čl. 18 odst. 1 písm. a) nařízení (EU) 2022/2554, zohlední finanční subjekt všechny dotčené transakce zahrnující peněžní částku, u nichž se alespoň jedna část transakce provádí v Unii.
5. Pokud nelze stanovit skutečný počet dotčených klientů nebo finančních protistran nebo skutečný počet či skutečnou výši dotčených transakcí, finanční subjekt tyto počty nebo výše odhadne na základě dostupných údajů za srovnatelná referenční období.

Článek 2

Poškození dobré pověsti

1. Pro účely stanovení toho, zda incident poškodil dobrou pověst, podle čl. 18 odst. 1 písm. a) nařízení (EU) 2022/2554 mají finanční subjekty za to, že k poškození dobré pověsti došlo, je-li splněno alespoň jedno z těchto kritérií:
 - a) incident byl zveřejněn v médiích;
 - b) incident měl za následek, že různí klienti nebo finanční protistrany opakovaně podávali stížnosti týkající se klientských služeb nebo zásadních obchodních vztahů;
 - c) finanční subjekt v důsledku incidentu nebude schopen nebo pravděpodobně nebude schopen splnit regulatorní požadavky;
 - d) finanční subjekt v důsledku incidentu přijde nebo pravděpodobně přijde o klienty nebo finanční protistrany, což bude mít významný dopad na jeho obchodní činnost.

⁽⁹⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

2. Při posuzování poškození dobré pověsti incidentem finanční subjekty zohlední, do jaké míry incident byl nebo pravděpodobně bude zviditelněn v souvislosti s jednotlivými kritérii uvedenými v odstavci 1.

Článek 3

Doba trvání incidentu a doba odstávky služby

1. Finanční subjekty měří dobu trvání incidentu uvedenou v čl. 18 odst. 1 písm. b) nařízení (EU) 2022/2554 od okamžiku výskytu incidentu do okamžiku jeho vyřešení.

Pokud finanční subjekty nejsou schopny určit okamžik výskytu incidentu, měří dobu trvání incidentu od okamžiku jeho detekce. Zjistí-li finanční subjekty, že k výskytu incidentu došlo ještě před jeho detekcí, měří dobu trvání od okamžiku, kdy byl incident zaznamenán v síťových nebo systémových protokolech nebo v jiných zdrojích údajů.

Pokud finanční subjekty prozatím neví, kdy bude incident vyřešen, nebo nemohou ověřit záznamy z protokolů nebo jiných zdrojů údajů, použijí odhady.

2. Finanční subjekty měří dobu odstávky služby způsobené incidentem uvedenou v čl. 18 odst. 1 písm. b) nařízení (EU) 2022/2554 od okamžiku, kdy je služba pro klienty, finanční protistrany nebo jiné interní či externí uživatele zcela nebo částečně nedostupná, do okamžiku, kdy jsou běžné činnosti nebo operace obnoveny na úroveň služby, která byla poskytována před incidentem. V případě, že je v důsledku odstávky služba poskytnuta se zpožděním poté, co byly běžné činnosti nebo operace obnoveny, měří se doba odstávky služby od začátku incidentu do okamžiku, kdy je daná zpožděná služba poskytnuta v plném rozsahu.

Pokud finanční subjekty nejsou schopny určit okamžik, kdy odstávka služby začala, měří dobu odstávky služby od okamžiku její detekce.

Článek 4

Územní rozsah

Pro účely stanovení územního rozsahu, pokud jde o oblasti dotčené incidentem, uvedeného v čl. 18 odst. 1 písm. c) nařízení (EU) 2022/2554 finanční subjekty posoudí, zda incident má nebo měl dopad v jiných členských státech, a zejména významnost tohoto dopadu ve vztahu ke kterémukoli z těchto subjektů:

- a) klienti a finanční protistrany v jiných členských státech;
- b) pobočky nebo jiné finanční subjekty v rámci skupiny, které vykonávají činnost v jiných členských státech;
- c) infrastruktury finančních trhů nebo poskytovatelé z řad třetích stran, kteří mohou mít vliv na finanční subjekty v jiných členských státech, jimž poskytují služby, a to v rozsahu, v jakém jsou takové informace k dispozici.

Článek 5

Ztráty údajů

Pro účely stanovení ztrát údajů, které incident způsobil, uvedených v čl. 18 odst. 1 písm. d) nařízení (EU) 2022/2554 finanční subjekty zohlední:

- a) pokud jde o dostupnost údajů, zda incident způsobil, že údaje poskytované na požádání finančního subjektu, jeho klientů nebo jeho protistran jsou dočasně nebo trvale nepřístupné nebo nepoužitelné;
- b) pokud jde o hodnověrnost údajů, zda incident narušil důvěryhodnost zdroje údajů;

- c) pokud jde o integritu údajů, zda incident vedl k neoprávněné změně údajů, v jejímž důsledku jsou nepřesné nebo neúplné;
- d) pokud jde o důvěrnost údajů, zda incident vedl k tomu, že k údajům získala přístup neoprávněná strana nebo neoprávněný systém nebo že byly údaje takové straně nebo takovému systému zpřístupněny.

Článek 6

Význam dotčených služeb

Pro účely stanovení významu dotčených služeb uvedeného v čl. 18 odst. 1 písm. e) nařízení (EU) 2022/2554 finanční subjekty posoudí, zda incident:

- a) má nebo měl dopad na služby IKT nebo síť a informační systémy, jež podporují zásadní nebo důležité funkce finančního subjektu;
- b) má nebo měl dopad na finanční služby, které finanční subjekt poskytuje a které vyžadují povolení, registraci nebo nad nimiž vykonávají dohled příslušné orgány;
- c) představuje nebo představoval úspěšný, zlovolný a neoprávněný přístup do sítě a informačních systémů finančního subjektu.

Článek 7

Ekonomický dopad

1. Pro účely stanovení ekonomického dopadu incidentu uvedeného v čl. 18 odst. 1 písm. f) nařízení (EU) 2022/2554 finanční subjekty zohlední bez započtení zpětně získaných finančních prostředků tyto druhy přímých a nepřímých nákladů a ztrát, které jim v důsledku incidentu vznikly:

- a) ztracené finanční prostředky nebo finanční aktiva, za které jsou odpovědné, včetně aktiv odcizených při krádeži;
- b) náklady na výměnu nebo přemístění softwaru, hardwaru nebo infrastruktury;
- c) náklady na zaměstnance, včetně nákladů spojených s výměnou nebo přeložením zaměstnanců, náborem dalších zaměstnanců, odměnou za práci přesčas a obnovou pozbytých nebo zhoršených dovedností;
- d) poplatky vzniklé nedodržením smluvních závazků;
- e) náklady na odčinění a náhradu újmy zákazníkům;
- f) ztráty vyplývající z ušlých příjmů;
- g) náklady spojené s interní a externí komunikací;
- h) náklady na poradenství, včetně nákladů spojených s právním poradenstvím, forenzními službami a službami k zajištění nápravy.

2. Náklady a ztráty uvedené v odstavci 1 nezahrnují náklady, které jsou nezbytné k zajištění každodenního provozu podniku, zejména:

- a) náklady na běžnou údržbu infrastruktury, zařízení, hardwaru a softwaru a náklady na udržování dovedností zaměstnanců na aktuálně potřebné úrovni;
- b) interní nebo externí náklady na posílení podniku po incidentu, včetně modernizací, zlepšení a iniciativ v oblasti posuzování rizik;
- c) pojistné.

3. Finanční subjekty vypočítají výši nákladů a ztrát na základě údajů, které mají k dispozici v době hlášení. Pokud nelze stanovit skutečnou výši nákladů a ztrát, finanční subjekty jejich výši odhadnou.

4. Při posuzování ekonomického dopadu incidentu finanční subjekty sečtou náklady a ztráty uvedené v odstavci 1.

KAPITOLA II

ZÁVAŽNÉ INCIDENTY A PRAHOVÉ HODNOTY VÝZNAMNOSTI

Článek 8

Závažné incidenty

1. Pro účely čl. 19 odst. 1 nařízení (EU) 2022/2554 se incident považuje za závažný incident, pokud jsou jím dotčeny významné služby podle článku 6 a pokud je splněna některá z těchto podmínek:

- a) je dosažena prahová hodnota významnosti uvedená v čl. 9 odst. 5 písm. b);
- b) jsou dosaženy dvě nebo více jiných prahových hodnot významnosti uvedených v čl. 9 odst. 1 až 6.

2. Opakující se incidenty, které samostatně nejsou považovány za závažné incidenty podle odstavce 1, se považují za jeden závažný incident, pokud splňují všechny tyto podmínky:

- a) došlo k nim nejméně dvakrát během šesti měsíců;
- b) mají tutéž zjevnou hlavní příčinu podle čl. 20 prvního pododstavce písm. b) nařízení (EU) 2022/2554;
- c) společně splňují kritéria pro to, aby byly považovány za závažný incident, stanovená v odstavci 1.

Finanční subjekty posuzují, zda se vyskytly opakující se incidenty, vždy měsíčně.

Tento odstavec se nepoužije na mikropodniky a na finanční subjekty uvedené v čl. 16 odst. 1 nařízení (EU) 2022/2554.

Článek 9

Prahové hodnoty významnosti pro stanovení závažných incidentů

1. Prahová hodnota významnosti u kritéria „klienti, finanční protistrany a transakce“ je dosažena, pokud je splněna některá z těchto podmínek:

- a) počet dotčených klientů je vyšší než 10 % všech klientů využívajících dotčenou službu;
- b) počet dotčených klientů využívajících dotčenou službu je vyšší než 100 000;
- c) počet dotčených finančních protistran je vyšší než 30 % všech finančních protistran, které vykonávají činnosti související s poskytováním dotčené služby;
- d) počet dotčených transakcí je vyšší než 10 % průměrného denního počtu transakcí prováděných finančním subjektem v souvislosti s dotčenou službou;
- e) výše dotčených transakcí je vyšší než 10 % průměrné denní hodnoty transakcí prováděných finančním subjektem v souvislosti s dotčenou službou;
- f) byli dotčeni klienti nebo finanční protistrany, kteří byli identifikováni jako významní v souladu s čl. 1 odst. 3.

Pokud nelze stanovit skutečný počet dotčených klientů nebo finančních protistran nebo skutečný počet či skutečnou výši dotčených transakcí, finanční subjekt tyto počty nebo výše odhadne na základě dostupných údajů za srovnatelná referenční období.

2. Prahová hodnota významnosti u kritéria „poškození dobré pověsti“ je dosažena, pokud je splněna některá z podmínek stanovených v čl. 2 písm. a) až d).

3. Prahová hodnota významnosti u kritéria „doba trvání incidentu a doba odstávky služby“ je dosažena, pokud je splněna některá z těchto podmínek:

- a) doba trvání incidentu je delší než 24 hodin;

- b) doba odstávky služby u služeb IKT podporujících zásadní nebo důležité funkce je delší než dvě hodiny.
4. Prahová hodnota významnosti u kritéria „územní rozsah“ je dosažena, pokud má incident dopad ve dvou nebo více členských státech v souladu s článkem 4.
5. Prahová hodnota významnosti u kritéria „ztráty údajů“ je dosažena, pokud je splněna některá z těchto podmínek:
- a) jakýkoli dopad na dostupnost, hodnověrnost, integritu nebo důvěrnost údajů uvedený v článku 5 má nebo bude mít nepříznivý dopad na plnění obchodních cílů finančního subjektu nebo na jeho schopnost splnit regulatorní požadavky;
 - b) došlo k jakémukoli úspěšnému, zlovolnému a neoprávněnému přístupu do sítě a informačních systémů, na který se nevztahuje písmeno a), může-li tento přístup vést ke ztrátám údajů.
6. Prahová hodnota významnosti u kritéria „ekonomický dopad“ je dosažena, pokud náklady a ztráty, které finančnímu subjektu v důsledku incidentu vznikly, přesáhly nebo pravděpodobně přesáhnou 100 000 EUR.

KAPITOLA III

VÝZNAMNÉ KYBERNETICKÉ HROZBY

Článek 10

Vysoké prahové hodnoty významnosti pro určování významných kybernetických hrozeb

Pro účely čl. 18 odst. 2 nařízení (EU) 2022/2554 se kybernetická hrozba považuje za významnou, pokud jsou splněny všechny tyto podmínky:

- a) podle informací, jež má finanční subjekt k dispozici, kybernetickou hrozbou, pokud by se naplnila, mohly být dotčeny nebo by mohly být dotčeny zásadní nebo důležité funkce finančního subjektu nebo by jí mohly být dotčeny jiné finanční subjekty, poskytovatelé z řad třetích stran, klienti nebo finanční protistrany;
- b) existuje vysoká pravděpodobnost, že se kybernetická hrozba naplní u finančního subjektu nebo u jiných finančních subjektů, a to při zohlednění alespoň těchto prvků:
 - i) příslušných rizik souvisejících s kybernetickou hrozbou uvedených v písmeni a), včetně potenciálních zranitelností systémů finančního subjektu, které mohou být zneužity;
 - ii) schopností a úmyslu aktérů hrozeb v rozsahu, v jakém jsou finančnímu subjektu známy;
 - iii) toho, zda hrozba přetrvává, a veškerých nashromážděných poznatků o incidentech, které měly dopad na finanční subjekt nebo jeho poskytovatele z řad třetích stran, klienty nebo finanční protistrany;
- c) kybernetická hrozba by v případě, že by se naplnila, mohla splňovat některou z těchto podmínek:
 - i) kritérium týkající se významu služeb stanovené v čl. 18 odst. 1 písm. e) nařízení (EU) 2022/2554 a upřesněné v článku 6 tohoto nařízení;
 - ii) prahovou hodnotu významnosti stanovenou v čl. 9 odst. 1;
 - iii) prahovou hodnotu významnosti stanovenou v čl. 9 odst. 4.

Dospěje-li finanční subjekt v závislosti na typu kybernetické hrozby a dostupných informacích k závěru, že by mohly být dosaženy prahové hodnoty významnosti stanovené v čl. 9 odst. 2, 3, 5 a 6, lze tyto prahové hodnoty rovněž zohlednit.

KAPITOLA IV

RELEVANTNOST ZÁVAŽNÝCH INCIDENTŮ PRO PŘÍSLUŠNÉ ORGÁNY V JINÝCH ČLENSKÝCH STÁTECH A ÚDAJE V HLÁŠENÍCH, KTERÉ JSOU SDÍLENY S DALŠÍMI PŘÍSLUŠNÝMI ORGÁNY

Článek 11

Relevantnost závažných incidentů pro příslušné orgány v jiných členských státech

Východiskem pro posouzení, zda je závažný incident relevantní pro příslušné orgány v jiných členských státech, podle čl. 19 odst. 7 nařízení (EU) 2022/2554 je to, zda se hlavní příčina incidentu nachází v jiném členském státě nebo zda incident má nebo měl v jiném členském státě významný dopad ve vztahu ke kterémukoli z těchto subjektů:

- a) klienti nebo finanční protistrany;
- b) pobočka finančního subjektu nebo jiný finanční subjekt v rámci skupiny;
- c) infrastruktura finančního trhu nebo poskytovatel z řad třetích stran, kteří mohou mít vliv na finanční subjekty, jimž poskytují služby.

Článek 12

Podrobnosti o závažných incidentech, které jsou sdíleny s dalšími příslušnými orgány

Podrobnosti o závažných incidentech, které příslušné orgány poskytují dalším příslušným orgánům v souladu s čl. 19 odst. 6 nařízení (EU) 2022/2554, a oznámení, která EBA, ESMA nebo EIOPA a ECB zasílají relevantním příslušným orgánům v jiných členských státech v souladu s čl. 19 odst. 7 uvedeného nařízení, musí obsahovat stejnou úroveň informací, bez jakékoli anonymizace, jako oznámení a zprávy o závažných incidentech obdržené od finančních subjektů v souladu s čl. 19 odst. 4 nařízení (EU) 2022/2554.

KAPITOLA V

ZÁVĚREČNÁ USTANOVENÍ

Článek 13

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 13. března 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN